Amendments to the claims

1 (Currently amended): A computer program, embodied on a computer readable storage medium, for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed, ~~the method~~ comprising:

a code segment that listens with a computerized system for an activation of the hyperlink;

a code segment that extracts an originator identifier and encrypted data from the hyperlink;

a code segment that decrypts said encrypted data into decrypted data based on said originator identifier;

a code segment that presents information on a display unit;

a code segment that redirects; and

a code segment that determines whether the hyperlink includes said originator identifier and said encrypted data decrypts successfully, and then:

runs said code segment that presents, to present a confirmation of authentication to the user conveying the name of ~~the~~ an owner and the domain name of the target URL, and

runs said code segment that redirects, to redirect the user to the target URL;

and otherwise, runs said code segment that presents, to present a warning dialog to the user.

2 (Original): The computer program of claim 1, wherein the computer program is digitally signed.

3 (Original): The computer program of claim 1, wherein said code segment that listens runs as a service in said computerized system.

4 (Original): The computer program of claim 1, wherein said code segment that listens includes a hypertext transport protocol (HTTP) server.

5 (Currently amended): The computer program of claim 1, wherein said code segment that

Amendments to the claims

listens ~~listens~~ at a preset ~~non routable~~ non-routable internet protocol (IP) address and at a preset port.

6 (Original): The computer program of claim 1, wherein said code segment that decrypts includes a code segment that extracts the target URL from said decrypted data.

7 (Original): The computer program of claim 1, wherein said the hyperlink includes the target URL and said code segment that decrypts includes:

a code segment that extracts a digital signature from said decrypted data; and

a code segment that verifies said digital signature against said originator identifier.

8 (Original): The computer program of claim 1, wherein said code segment that decrypts employs a public key associated with said originator identifier.

9 (Original): The computer program of claim 1, further comprising:

a code segment that matches said originator identifier to one of a plurality of registered originators; and

a code segment that retrieves a decryption key associated with said originator identifier for use by said code segment that decrypts.

10 (Original): The computer program of claim 1, wherein said code segment that presents employs a dialog box that only software running locally in said computerized system can provide, thereby avoiding confusion with a remotely generated browser window.

11 (Currently amended): A system for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed, the system comprising:

a computerized system having a display unit;

a logic in said computerized system that listens for activation of the hyperlink;

a logic that extracts an originator identifier and encrypted data from the hyperlink;

a logic that decrypts said encrypted data into decrypted data based on said originator

Amendments to the claims

identifier;

a logic that determines whether the hyperlink includes said originator identifier and that said encrypted data decrypts successfully;

a logic responsive to said logic that determines, that presents on said display unit a confirmation of authentication conveying the name of ~~the~~ an owner and the domain name of the target URL and that redirects the user to the target URL; and

a logic responsive to said logic that determines, that presents on said display unit a warning dialog to the user.

12 (Original): The system of claim 11, wherein said logic that listens runs as a service.

13 (Original): The system of claim 11, wherein logic that listens includes a hypertext transport protocol (HTTP) server.

14 (Currently amended): The system of claim 11, wherein said logic that listens ~~listens~~ at a preset ~~non-routable~~ non-routable internet protocol (IP) address and at a preset port.

15 (Original): The system of claim 11, wherein said logic that decrypts includes a logic that extracts the target URL from said decrypted data.

16 (Original): The system of claim 11, wherein said the hyperlink includes the target URL and said logic that decrypts includes:

a logic that extracts a digital signature from said decrypted data; and

a logic segment that verifies said digital signature against said originator identifier.

17 (Original): The system of claim 11, wherein said logic that decrypts employs a public key associated with said originator identifier.

18 (Original): The system of claim 11, further comprising:

a logic that matches said originator identifier to one of a plurality of registered

Amendments to the claims

originators; and

a logic that retrieves a decryption key associated with said originator identifier for use by said logic that decrypts.

19 (Original): The system of claim 11, wherein said logic that presents employs a dialog box that only software running locally in said computerized system can provide, thereby avoiding confusion with a remotely generated browser window.

20 (Currently amended): A method for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed, the method comprising:

listening for an activation of the hyperlink;

extracting an originator identifier and encrypted data from the hyperlink;

decrypting said encrypted data into decrypted data based on said originator identifier;

when the hyperlink includes said originator identifier and said encrypted data decrypts successfully:

presenting a confirmation of authentication to the user, wherein said confirmation of authentication conveys the name of ~~the~~ an owner and the domain name of the target URL; and

redirecting the user to the target URL;

and otherwise, presenting a warning dialog to the user.

21 (Original): The method of claim 20, wherein said listening includes running at least one of a service and a hypertext transport protocol (HTTP) server in a computerized system.

22 (Currently amended): The method of claim 20, wherein said listening is at a preset ~~non routable~~ non-routable internet protocol (IP) address and a preset port.

23 (Original): The method of claim 20, said decrypting includes extracting the target URL from said decrypted data.

Amendments to the claims

24 (Original): The method of claim 20, wherein said the hyperlink includes the target URL and said decrypting includes:

extracting a digital signature from said decrypted data; and

verifying said digital signature against said originator identifier.

25 (Original): The method of claim 20, further comprising:

matching said originator identifier to one of a plurality of registered originators;

retrieving a decryption key associated with said originator identifier for use in said decrypting.

26 (Original): The method of claim 20, wherein said presenting a confirmation employs a dialog box that only software running locally in a computerized system can provide, thereby avoiding confusion with a remotely generated browser window.